



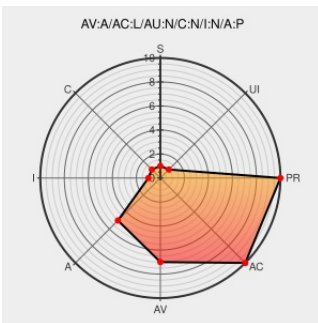
Last Modified on: 03/23/2021 11:28:42 PM UTC

CVE-2013-2479

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Opensuse](#) from [Opensuse](#) contain the following vulnerability:

The `dissect_mpls_echo_tlv_dd_map` function in `epan/dissectors/packet-mpls-echo.c` in the MPLS Echo dissector in Wireshark 1.8.x before 1.8.6 allows remote attackers to cause a denial of service (infinite loop) via invalid Sub-tlv data.

CVE-2013-2479 has been assigned by  cve@mitre.org to track the vulnerability

CVSS2 Score: 3.3 - LOW

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-mpls-echo.c?r1=46391&r2=46390&pathrev=46391
Security Advisory SA52471 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia	web.archive.org text/html	 SECUNIA 52471
openSUSE-SU-2013:0494-1: moderate: wireshark: update to 1.8.6	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0494
Bug 8039 – MPLS infinite loop	bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=8039
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=46391
Wireshark · wnpa-sec-2013-14 · MPLS Echo	Vendor Advisory	 CONFIRM www.wireshark.org/security/wnpa-sec-2013-

dissector infinite loop	www.wireshark.org text/html	14.html
openSUSE-SU-2013:0506-1: moderate: wireshark: update to 1.8.6	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0506
Wireshark · Wireshark 1.8.6 Release Notes	www.wireshark.org text/html	 CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.6.html
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org/mitre.oval:def:16376

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All

Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
cpe:2.3:o:opensuse:opensuse:11.4:*****:						
cpe:2.3:o:opensuse:opensuse:12.1:*****:						
cpe:2.3:o:opensuse:opensuse:12.2:*****:						
cpe:2.3:o:opensuse:opensuse:12.3:*****:						
cpe:2.3:o:opensuse:opensuse:11.4:*****:						
cpe:2.3:o:opensuse:opensuse:12.1:*****:						
cpe:2.3:o:opensuse:opensuse:12.2:*****:						
cpe:2.3:o:opensuse:opensuse:12.3:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.0:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.1:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.2:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.3:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.4:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.5:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.0:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.1:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.2:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.3:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.4:*****:						
cpe:2.3:a:wireshark:wireshark:1.8.5:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)